DATE(S) ISSUED:
05/08/2012

SUBJECT:
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (MS12-035)

OVERVIEW:
Two vulnerabilities has been discovered in the Microsoft .NET Framework which could allow an attacker to take complete control of an affected system. Microsoft .NET is a software framework for applications designed to run under Microsoft Windows. These vulnerabilities can be exploited if a user visits or is redirected to a malicious web page, or runs a specially crafted Microsoft .NET application.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
· Microsoft .NET Framework 1.0 SP3
· Microsoft .NET Framework 1.1 SP1
· Microsoft .NET Framework 2.0 SP2
· Microsoft .NET Framework 3.0 SP2
· Microsoft .NET Framework 3.5 SP1
· Microsoft .NET Framework 4.0

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Two vulnerabilities have been discovered in the Microsoft .NET Framework that could allow an attacker to take complete control of an affected system. These vulnerabilities are caused due to .NET improperly handling an exception during the object serialization process. These vulnerabilities can be exploited in any of the following scenarios:

In the first scenario, exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content.

In the second scenario, an attacker can exploit these issues by creating a specially crafted Windows .NET application to bypass Code Access Security (CAS) restrictions.

Successful exploitation of these scenarios could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
·   Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
·   Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
·   Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
·   Unless there is a business need to do otherwise, consider disabling XAML browser applications (XBAP) in Internet Explorer.

REFERENCES:
Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms12-035

Security Focus:
http://www.securityfocus.com/bid/53356
http://www.securityfocus.com/bid/53357

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0160
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0161